



SWITCH

The Swiss Education & Research Network

The WAYF and the Resource Registry

Thomas Lenggenhager
lenggenhager@switch.ch

- WAYF - Where are you from?
- Alternatives to centralized WAYF
- The WAYF in SWITCHaai
 - High Availability for the WAYF
 - Availability Monitoring and Control
 - Identity Provider Pre-selection
- Resource Registry
A tool to manage metadata

SWITCH^{aai}

[About AAI](#) : [About SWITCH](#) : [FAQ](#) : [Help](#) : [Privacy](#)

Select your SWITCH^{aai} Home Organization

In order to access a Resource on host 'kelut.switch.ch' you must authenticate yourself.

Select the Home Organization you are affiliated with ...

Remember selection for this web browser session.

- ▶ SWITCH recommends [importing the 'SwissSign Root CA Certificate'](#) into your web browser. That way, your web browser can seamlessly establish secure connections to AAI-enabled web servers.
- ▶ The [SWITCH](#) Foundation operates the Swiss Education & Research Network which guarantees high-speed connectivity to the Internet and to science networks globally for the benefit of higher education in Switzerland.

⇒ **Task of WAYF is to guide user to his Identity Provider**





Facts about WAYF

- Stateless requests
- Two requests per visit
 1. Show drop-down list
 2. Redirect User to IdP



The Internet2 WAYF

- It is part of the Shibboleth IdP package, implemented in JSP.

<h3>Select an Identity Provider</h3>	<h3>Select an Identity Provider</h3>
<p>In order to fulfill the request for a web resource you have just attempted to access, information must be obtained from your identify provider. Please select the provider with which you are affiliated.</p>	<p>In order to fulfill the request for a web resource you have just attempted to access, information must be obtained from your identify provider. Please select the provider with which you are affiliated.</p>
<p>Choose from a list:</p>	<p>Choose from a list:</p>
<p>AAI EDUHR TEST <input type="button" value="Select"/> <input type="button" value="Remember"/></p>	<p>Case Western Reserve University <input type="button" value="Select"/> <input type="button" value="Remember for session"/></p>
<p>or</p>	<p>or</p>
<p>Search by keyword:</p>	<p>Search by keyword:</p>
<p><input type="text"/> <input type="button" value="Search"/></p>	<p><input type="text"/> <input type="button" value="Search"/></p>
<p>Find out about InQueue.</p> <p>Got here by mistake? Don't see a suitable or recognizable id list? Just use your browser's Back button to return to the page here.</p>   	<p>If you are having trouble accessing a resource via InCommon please check that your organization is an InCommon Participant and offers the resource you are trying to visit. For assistance please contact the resource provider or your home organization.</p> <p>If you were unable to find your organization in the InCommon WAYF pull down list, please visit the InCommon participants page to verify if your organization participates in InCommon.</p> 

Three ways to become independent of central WAYF

- A single Identity Provider to support
 - Link directly to the Identity Provider
set `wayfURL` in `shibboleth.xml` to `providerId` of IdP

- Only few Identity Providers
 - Offer direct – ‘bookmarkable’ – links to IdPs

<https://idp.xy.org/shibboleth-idp/SSO?shire=...&providerId=...&target=...>

⇒ ‘Shibboleth Architecture Protocols and Profiles’ document
in chapter 3.1.1 ‘Authentication Request Profile’

- Integrate WAYF into the Service Provider
 - Use your own WAYF
⇒ examples on next slides

Integrated WAYF: OLAT

- WAYF integrated into an Open source e-learning platform (= LMS = VLE)
- <http://olat.unizh.ch>

The screenshot shows the OLAT login interface. At the top, there is a language selection bar with options for Deutsch, English, Français, Italiano, and Help. Below this, the page title is "OLAT - Online Learning And Training". On the left side, there is a navigation menu with links for "OLAT Login", "Guest access", "Browser check", "About cookies", and "About OLAT". The main content area features the OLAT logo and a message: "Please select your university. You will be redirected for authentication." Below this message is a dropdown menu for "University:" with "Université de Fribourg - Universität Freib" selected. A "Login" button is positioned below the dropdown. At the bottom of the main content area, there are links for "Gastzugang" and "Forgot your password?". Below the main content area, there is a section titled "Alternative login possibilities." with the text "Do you not belong to one of the abovementioned universities?" and a "Continue" link.

Integrated WAYF: ScienceDirect

- <http://www.sciencedirect.com>

ELSEVIER SCIENCE @ DIRECT

[Register](#) or Login: user name Password: [Athens/Institution Login](#)

Quick Search: within WELCOME GUEST

Full-text articles in ScienceDirect: 7,242,819

ScienceDirect Info

- [About ScienceDirect](#)
- [Content Coverage](#)
- [Librarian Services](#)
- [Guest User Info](#)
- [About Athens](#)

Why Register?
[User Guides](#)

ScienceDirect News
[Contact Us](#)
[More Info...](#)

ScienceDirect®

Welcome to the world's largest electronic collection of science, technology and medicine full text and bibliographic information.

Elsevier Admin Tool
The best way to manage your ScienceDirect account. [Learn more...](#)

Over 1800 titles online...

Search for a Title:

OR [Browse A-Z](#)

Subject Areas in ScienceDirect

- [Agricultural and Biological Sciences](#)
- [Arts and Humanities](#)
- [Biochemistry, Genetics and Molecular Biology](#)
- [Business, Management and Accounting](#)

Integrated WAYF: ScienceDirect (2)

- First choose the federation...

The screenshot shows the ScienceDirect website interface. At the top left is the Elsevier logo. To its right is the text "SCIENCE @ DIRECT". Further right is a registration and login area with the text "Register or Login:" followed by a "user name" input field, a "Password:" input field, a "Go" button, and a link for "Athens/Institution Login". Below this is a navigation bar with buttons for "Home", "Journals", "Books", "Abstract Databases", "My Profile", and "Alerts", along with a "Help" link. At the bottom of the navigation bar is a "Quick Search:" input field, a "within" dropdown menu set to "All Full-text Sources", a "Go" button, a "Search Tips" link, and a "WELCOME GUEST" message.

Login via Athens or Your Institution

You may be able to login to ScienceDirect using Athens or your institution's login credentials. We will remember your login preference the next time you access ScienceDirect from this machine.

If you are an Athens user, please select the link below.

[Athens Login](#)

To login using your institution's login credentials, select a region or group.

Select your region or group

[View All Institutions](#)

Integrated WAYF: ScienceDirect (3)

- ...then choose the IdP

Login via Athens or Your Institution

You may be able to login to ScienceDirect using Athens or your institution's login credentials. We will remember your login preference the next time you access ScienceDirect from this machine.

If you are an Athens user, please select the link below.

[Athens Login](#)

To login using your institution's login credentials, select a region or group.

US Higher Education

Go

[View All Institutions](#)

Please choose one of the institutions listed below:

If your institution is not listed, it is not enabled for this type of login. Please contact your Librarian or Information Specialist.

US Higher Education

- [Dartmouth College](#)
- [The State University of New York at Buffalo](#)
- [University of California-San Diego](#)

- High Availability for the WAYF
 - Redundancy at two distant locations
 - IP Anycast
- Availability Monitoring and Control
- Identity Provider Pre-selection
- Features of the PHP WAYF

How to achieve High Availability

Answer: Redundancy

- Stateless services like the WAYF can be easily made redundant

Main Problems

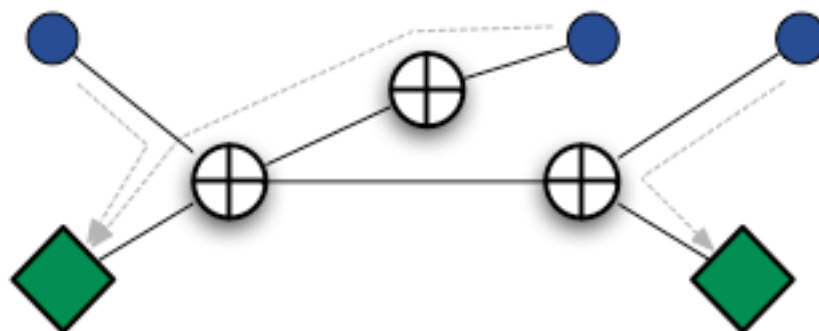
- 1) How to determine when failover situation occurs?
- 2) How to handle a failover situation?

Failover Handling

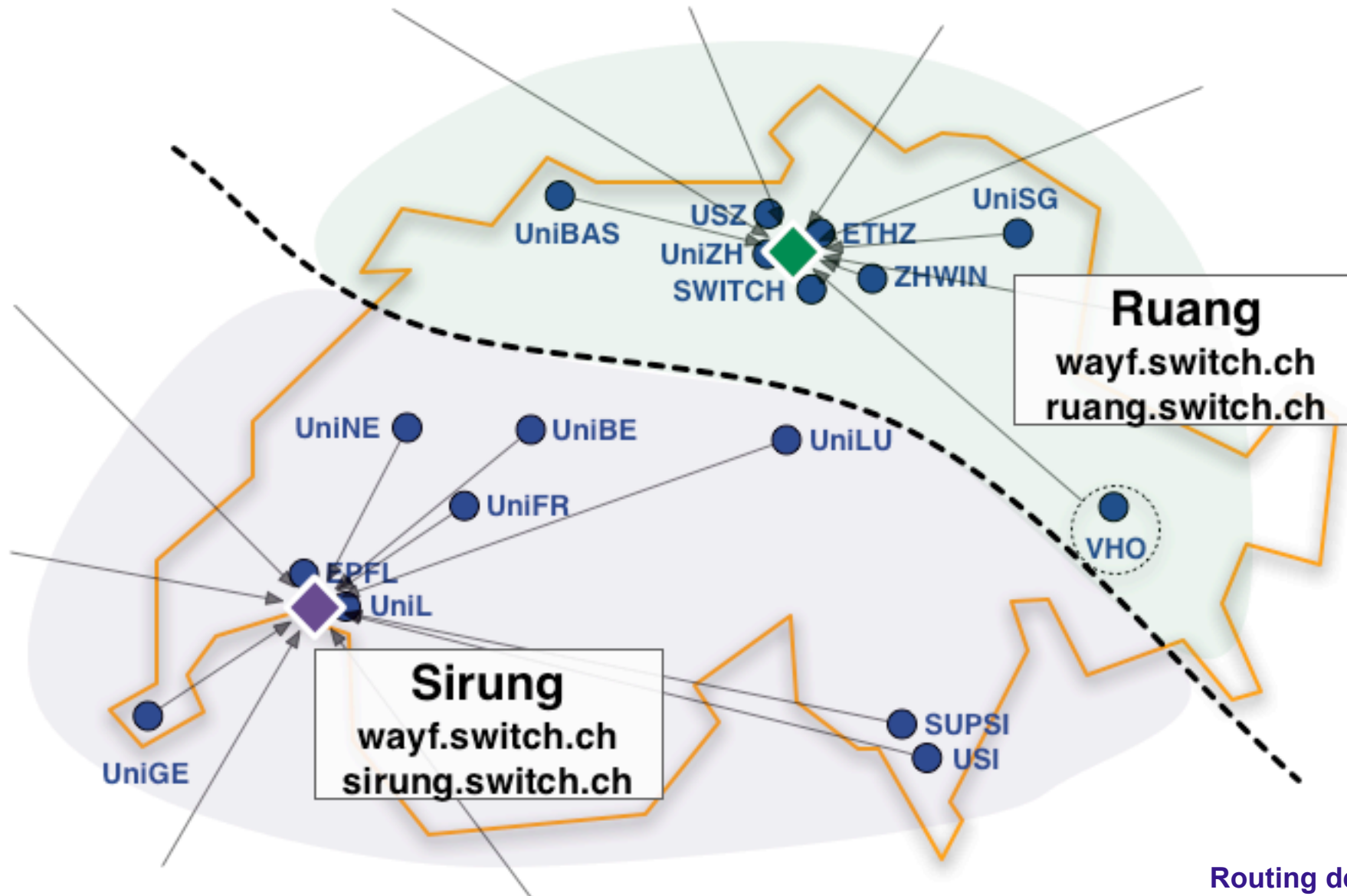
- Use DNS record to switch hosts
- Hide service behind load balancer
- Use master/slave services that share same IP
- Use Anycast (only recommended for specific services)

- Best suited for connection-less applications
- Used for DNS system of Root Servers (DNS queries mostly UDP)
- WAYF is stateless and routing within backbone is very constant
- Anycast is implemented using routing system
- Request to an IP is routed to the 'nearest' Anycast instance
- Changes propagate within seconds (~ 3s)

⇒ **Results in High Availability and Load Balancing**



Load Balancing Effect



Routing dependent

From inside the backbone

- Internal Big Brother (e-mail notification)

From outside the backbone

- Alertra.com (e-mail notification)

On WAYF Instance

- Routing Daemon Zebra/Quagga announces IP
- WAYFcheckservice script (e-mail notification and failover actions)
 - Polls service every minute. In case of problems tries to restart service.
 - If it fails, the Anycast IP announcement gets stopped immediately.
 - If host stops working before withdrawing route to Anycast IP (e.g. hardware failure, ...) remaining hosts take over within max. 40 seconds.

Goal

- at most one click per session for IdP selection

Two Cookies used

- Short term: Optionally skipping WAYF for current browser session
- Long term: Remembers past choices (100 days).
Useful for IdP pre-selection in next sessions.

Resource hints the WAYF with URN

- Append part of the providerID (URN) to WAYF URL
<https://wayf.switch.ch/SWITCHaai/WAYF/unige.ch?shire=...>

Transparent mode – Users never see the WAYF (limited use case)

- Append 'redirect' to WAYF URL
<https://wayf.switch.ch/SWITCHaai/WAYF/redirect/unizh.ch?shire=...>

Features of the PHP WAYF

- Enhanced ease-of use for the user
- Light-weight implementation of a WAYF service
- Implemented in PHP
- Multilingual based on browser setting
currently supported: en, fr, de, it
- Ready for push-update from Resource Registry (not yet used)
- OpenSource (BSD License)

- Interested? Contact aai@switch.ch

- Why a Resource Registry?
 - It's a tool to manage metadata
- Roles in the Resource Registry
 - Home Organization Administrator
 - Resource Registration Authority (RRA) Administrator
 - Resource Administrator
- Resource Registry User Guide
 - <http://www.switch.ch/aai/docs/AAI-RR-Guide.pdf>
- <https://aai-rr.switch.ch/>

Why a Resource Registry?

- Federation Metadata requires some config details
 - **Identity Provider** needs
 - metadata.xml: details of SPs
 - arp.sites.xml: attribute requirements of SPs
 - **Service Provider** needs
 - metadata.xml: details of IdPs
 - **WAYF** needs
 - list of all Identity Providers
- Home Organizations want to know about SPs in their domain
 - Resource Registration Authority (RRA)
- Resource Registry supportive, not to be operationally required
 - no potential central point of failure for end-user operations

1) AAI user account required

- First user of a Home Organization becomes its first Admin and first Resource Registry Authority (RRA) Admin

1) Enter details about the Home Organization

- Name, description, contact addresses
- Config details
 - like providerId, SSO and AA URLs
- Mark attributes implemented by the Home Organization
- Default attribute release preferences
 - Accept which required and desired attributes

2) Submit entry for approval to SWITCHaa Admins

Home Organization Administrator (2)

- 4) Delegate modification rights to other users
 - as Home Organization Admin and
 - as Resource Registration Authority (RRA) Admin

- 5) Retrieve tailored `arp.sites.xml`
 - Just the Resources of interest for this Home Organization
 - Based on Resource requirements and default attribute release preferences
 - `updateARP` Perl script provided for simple post-processing for the IdP
 - Block an attribute for a specific resource
 - Allow an attribute for a specific resource

- 1) AAI user account required
 - User gets this right from a Home Organization Admin

- 2) Approve Resources on behalf of Home Organization
 - Gets notification by e-mail on creation and modification
 - Should check the Resource details as provided, especially the attribute requirements
 - Should make Resource Admin aware of Federation Policy
 - Approves Resource

- 3) Delegate modification rights to other users
 - as Resource Registration Authority (RRA) Admin

- 1) AAI user account required
 - If Home Organization already registered the user gets accepted
- 2) Enter details about the Resource
 - Name, description, contact addresses
 - Config details
 - like providerId, shireURL, certificate subject name
 - Attribute requirements
 - required vs. desired with reason
 - Home Organization use
 - Resource of interest for which Identity Providers
- 3) Submit entry for approval to RRA
- 4) Delegate modification rights to other users
- 5) Each modification requires again RRA approval

Resource Registry: Details

- Tailored for SWITCHaai federation
 - grows with additional requirements
 - probably of limited direct use for other federations
not really configurable, many things hard coded
- Implemented in PHP using PEAR/QuickForm and MySQL
- OpenSource (BSD license)
- Available as is...

- Interested? Contact aai@switch.ch